ما هو ميتاسبلويت (Metasploit) ؟

تعريف الميتاسبلويت

كيف تعمل أداة الميتاسبلويت؟

كيفية التأكد من أن الهدف المستهدف نستطيع تنفيذ الهجوم عليه؟

ما معنى كلمة بيلود؟

أوامر الميتاسبلويت

كيفية تثبيت أداة Metasploit

تعريف الميتاسبلويت

عبارة عن مشروع ضخم يستخدم من قبل المتخصصين بمجال الإختراق الأخلاقي و أمن المعلومات حيث Metasploit أداة يمكن من خلالها البحث عن الثغرات الأمنية الموجودة في السيرفرات و الأجهزة و لهذا يتم إستغلال هذه الأداة أيضاً للقيام بعمليات غير شرعية و هذا الشائع للأسف.

إذاً هذه الأداة تعتبر سلاح فعال سواء بيد من يستخدمها بشكل أخلاقي أو غير أخلاقي و حتى للأغبياء أيضاً.

في هذا المقال سنتعرف على كيفية عمل هذه الأداة بشكل عام و كيفية تثبيتها على نظام لينكس, ويندوز و إندرويد.

كيف تعمل أداة الميتاسبلويت؟

إذا كنت ستستخدمها في إختبار إختراق شيء ما فيمكن تلخيص عملها كالتالي:

1- إختيار إحدى الثغرات المتوقعة و المتواجدة في الأداة و التي يتجاوز عددها 1500 ثغرة مثل ثغرة CVE_2017_8464 التي فقط و هذا مثال لها في يوتيوب (USB) تمكننا من إستهداف نظام ويندوز عبر فلاشة

2- يجب أن نتحقق من أن الهدف المستهدف نستطيع تطبيق هذه العملية عليه.

3- إختيار البيلود (Payload) المناسب للهدف.

4- إختيار تشفيرة مناسبة للبيلود لكي تتجاوز بها أنظمة الحماية.

5- تنفيذ الهجمة Run.

كيفية التأكد من أن الهدف المستهدف نستطيع تنفيذ الهجوم عليه؟

في حال كان الضحيه جهاز نقوم بإرسال رابط للضحية لجلب عنوانه (IP Address) أو جلب العنوان بواسطة أداة Etherape في حال وجود بورت يمكن إستغلاله نبدأ بالعملية, أما في حال Armitage أو أداة nmap و من ثم فحص هذا العنوان عبر أداة Ngrok أو غيرها من الأدوات التي يمكن أن تساعدنا لهذا الغرض, و من ثم تتم عمليه الإستهداف لم نجد بورت يمكن التسلل عبره يمكن فتح بورت لدى الضحية بإستعمالنا أداة.

ما معنى كلمة بيلود؟

كلمة بيلود (Payload) معناها التحميل الزائد باللغة العربية.

في مجال الشبكات معناها البيانات التي يستقبلها المستخدم بدون البيانات التي تكون موضوعة في هيدر الباكيت.

في مجال الأمن المعلوماتي تعني هو برمجية خبيثة يرسلها المخترق للضحية لفتح نافذه تواصل (بورت) بين الطرفين و هذا المعنى الذي نقصده منها في هذا المقال.

أوامر الميتاسبلويت

هو أمر فتح الأداة msfconsole.

هو أمر المساعدة الذي يمكنك من خلاله معرفة جميع الأوامر المتوفرة و كيفية التعامل معها help.

لمسح ما تم كتابته مسبقاً على الشاشة و جعلها فارغة clear.

يعرض لنا جميع الثغرات الموجودة في الميتاسبلويت حيث يعرض لنا أسماء الثغرات و تاريخ إكتشافها و show exploits بعض المعلومات الأخرى.

يعني إستغلال, عند البدء بإختيار ثغرة معينة نكتب بعده مسار الثغرة و إسمها ليتم إستغلالهما عند تنفيذ الهجمة use.

لعرض خيارات الثغرة و متطلبات الإستغلال show options.

لتعيين قيمة من متطلبات الثغرة مثلاً لتضع رقم البورت و إسم الهوست SET.

تعني تنفيذ الهجمة و هي تعني أن تفعل exploit Run.

لمعرفة الأهداف التي ستستهدفها الثغرة show target.

تعني الجلسات, و هذا الأمر يأتي بعد عملية الإستغلال يكون أي أن جلسه الإختراق قائمة و تعمل بنجاح. إذا أعطتك sessions فهذا يعني أن الجلسه غير متصلة أو كانت قائمة و انفصلت session not respond.

لعرض البيلودات و توجد أنواع كثيرة جداً و الأكثر إستخداماً هو show payloads meterpreter.

show encoders يعرض لنا الخوارزميات التي يمكن إستخدامها لتشفير البيلود حتى لا تكتشفه أنظمة الحماية.

كيفية تثبيت أداة Metasploit

سنشرح كيفية تثبيتها و فتحها على نظامي لينكس و ويندوز.

لمستخدمي نظام لينكس

هذه الأداة تكون مثبتة مسبقاً في أنظمة لينكس. لإيجاد الأداة علينا البحث عنها بين الأدوات الرسومية أو إستدعائها بالتيرمنال من خلال كتابة الأمر msfconsole.

ملاحظة: يجب أن ننتظر قليلاً و سوف تفتح لدينا الأداة بشكل طبيعي كالتالي:

مسار الميتاسبلويت في لينكس الذي يتيح لك الإطلاع على مجلدات الثغرات, الأنظمة و الإستغلالات هو التالي:

home/usr/share/metasploit-framework/modules/exploits

الصورة التالية التالية تظهر محتوى المجلد exploits

نلاحظ أن جميع ملفات الثغرات الذي به إمتدادها rb مما يعني أنها مبرمجة بلغة Ruby.

لمستخدمي نظام الويندوز

و نختار النسخة المناسبة للجهاز download نقوم بالتوجه للموقع الرسمي للأداة و نضغط على.

و ننتظر لحين إكمال تحميل الملف و تثبيته كتثبيت أي برنامج على الويندوز و فتحه.

لمستخدمي نظام إندرويد

بواستطه بكل سهولة Metasploit على نظام إندرويد فيمكنك تحميل الحزم المطلوبة لتثبيت Termux إذا كنت تستخدم برنامج
من خلال الأوامر التالية:

apt update

apt upgrade -y

pkg install ruby

pkg install unstable-repo

pkg install metasploit -y

.بعد كتابة الأمر الأخير تنتظر قليلاً على حسب سرعة الإنترنت لديك ريثما يتم تثبيتها

.و عندها ستفتح كالتالي كما تفتح في نظام لينكس msfconsole في النهاية تقوم بفتح الأداة بكتابة الأمر

لاختراق هو الدخول غير المشروع إلى جهاز حاسب ما عن طريق ثغرات في نظام الحماية باستخدام برامج متخصصة، يقوم بها .محترفون أو هواة، وذلك للحصول على البيانات أو العبث بها أو تدميرها

كيف يتم الاختراق؟

يتم اختراق الأجهزة بمعرفة الثغرات الموجودة في ذلك النظام كمنافذ الجهاز ، وذلك بطرق متعددة كإرسال ملف تجسس، علما أن .جميع الأنظمة الموصولة بالشبكات عرضة للاختراق

:طرق الاختراق

مجسات المنافذ. هذه البرامج تعمل على تحسس المنافذ غير المحمية للحواسيب المرتبطة بالإنترنت، فإذا ما وجدت ذلك دخلت .عبره إلى موارد الجهاز

.برامج إدارة الأجهزة عن بعد. وهي برامج أعدت للمساعدة لكنها قد تستغل استغلالاً سيئا

.أحصنة طروادة. برامج صغيرة تركب على الجهاز تفتح منافذ الجهاز للمخترق

.الحرمان من الخدمة. عبر إغراق الجهاز الموصول بكم هائل من البيانات بما يسبب له الانهيار

تشمم الرزم. وذلك عبر تفحص أي رزمة معلومات مرسلة من الحاسب المقصود للاطلاع على محتوياته، ولا مجال للمرسِل .لمعرفة الاختراق الذي وقع عليه

.استغلال ثغرات البرامج. يعمد المخترقون إلى معرفة ثغرات البرامج كنظام التشغيل مثلاً فيدخلون عبرها

برامج التجسس. هذه البرامج ترسل معلومات بشكل دوري عن عاداتك في استخدام الجهاز، والمواقع التي تزورها، والبرامج .التي تستخدمها، ومعلوماتك الشخصية

:أنواع الاختراق

.اختراق المزودات أو الأجهزة الرئيسية للمؤسسات

.اختراق الأجهزة الشخصية والعبث بما تحويه من معلومات

.اعتراض البيانات أثناء انتقالها بالشبكات

.تشويه مواقع الانترنت بتغيير محتواها

.هجمات حجب الخدمة

:أسباب الاختراق

.أسباب سياسية هجمات ضد موقع حكومي يتبع دولة ما أو موقع مؤسسة تنتمي إلى هذه الدولة

.أسباب اقتصادية كالمنافسة التجارية غير الشريفة

.الانتقام، فقد يلجأ بعض الذين يشعرون بالظلم إلى الانتقام من مؤسساتهم

.الطبيعة التخريبية وذلك لإشباع رغبات تخريبية تتملك المخترقين

.انتشار البرامج المساعدة وكثرتها وسهولة التعامل معها

.ارتفاع أسعار برامج وتطبيقات الحاسب الأصلية التي تنتجها الشركات

:أضرار الاختراق

.مخالفة القانون والتعرض للمساءلة

.الإضرار بسمعة الجهة المالكة

.مضيعة للموارد

.إهدار للوقت

كيف تواجه الاختراق؟

نصِّب برنامج جدار ناري.

نصِّب مضاد جيد للفيروسات.

حدِّث أنظمة الحماية بشكل دوري.

حدِّث برامج التشغيل وغيرها بشكل دوري لإغلاق ثغراتها.

غيِّر كلمة المرور بشكل دوري.

الهواتف المحمولة واحدة من أكثر الأجهزة استخدامًا في العالم، ولكنها في الوقت نفسه تشكل تحديًا كبيرًا فيما يتعلق بالأمان والحفاظ على الخصوصية.

وقد تم تطوير العديد من الأدوات والطرق المختلفة لاختراق الهواتف المحمولة، ولكن هناك أخطرها والذي يشكل تهديداً حقيقياً لبياناتك وخصوصيتك، وفيما يلي نستعرض بعضًا من أخطر هذه الطرق:

1. البرمجيات الخبيثة (Malware):

تُعد البرمجيات الخبيثة واحدة من أخطر الأدوات التي يمكن استخدامها لاختراق الهواتف المحمولة. وتتمثل هذه البرمجيات في برامج تم تصميمها للدخول إلى الهاتف والتحكم فيه دون علم صاحب الجهاز. ويمكن أن تأتي هذه البرامج عبر رسائل البريد الإلكتروني المزيفة، (SMS) أو رسائل النص القصير، أو التطبيقات المزيفة.

2. الاستنساخ الهجين (Hybrid Cloning):

يستخدم هذا النوع من الاختراق في الغالب في أنشطة التجسس أو التجسس الصناعي، حيث يتم إنشاء نسخة من الهاتف المحمول

المستهدف واستخدامها للوصول إلى المعلومات المخزنة على الجهاز الأصلي. ويتم ذلك من خلال تثبيت برمجية معينة على الهاتف الهدف تتيح للمهاجم الوصول إلى المعلومات المخزنة عليه.

3. الهجوم بواسطة الـ SS7:

يعتمد هذا الهجوم على استغلال ضعف في نظام الإشارة 7 (SS7) الذي يسمح بتحويل المكالمات والرسائل النصية بين مزودي خدمات الاتصالات المختلفة. ويمكن للمهاجم استخدام هذا الضعف للوصول إلى المعلومات المخزنة على الهاتف المحمول، وحتى السيطرة على الجهاز.

4. الاستغلال المتقدم للثغرات الأمنية:

يتم استخدام هذا النوع من الاختراق في الغالب من قبل المحترفين والمتخصصين في مجال الأمن السيبراني. ويتم ذلك عن طريق استغلال الثغرات الأمنية في نظام التشغيل أو التطبيقات المختلفة على الهاتف المحمول، ويمكن للمهاجم من خلال ذلك الوصول إلى المعلومات المخزنة على الجهاز.

5. الهجمات المستهدفة (Targeted Attacks):

يتم استخدام هذا النوع من الاختراق في الغالب في أنشطة التجسس والتجسس الصناعي، حيث يتم استهداف شخص معين أو مجموعة محددة من الأفراد. ويتم ذلك من خلال إرسال رسائل مزيفة أو روابط مشبوهة، أو استخدام تطبيقات مزيفة للحصول على المعلومات المطلوبة.

هذا ويجب على المستخدمين اتخاذ الإجراءات اللازمة لحماية الهواتف المحمولة من هذه الطرق الخبيثة، وذلك من خلال تحديث البرامج والتطبيقات بانتظام، وتفعيل الحماية بكلمة مرور قوية، وتجنب تحميل التطبيقات من مصادر غير موثوقة، وعدم الاستجابة للرسائل النصية أو البريد الإلكتروني المشبوه، والابتعاد عن الاتصال بالشبكات العامة غير المشفرة.

حل مشكلة الميتاسبلويت

في الحل الأول واجه البعض من المشاكل وتكررت المشكلة عند الناس ولم يستطيعوا تنزيل الميتاسبلويت علي الترمكس.. لذلك اليوم احضرت لكم حل اخر لهذه المشكلة وتثبيت الميتاسبلويت اخر اصدار

الأوامر

pkg update && pkg upgrade

git clone https://github.com/noob-hackers/m-wiz

cd m-wiz

chmod +x m-wiz.sh

bash m-wiz.sh

Enter ثم نضغط

ثم نختار رقم 1

Enter ثم نضغط

ثم نختار رقم 2

وبعد الأنتهاء من التثبيت ستدخل مباشرة علي الميتاسبلويت

للدخول مرة اخرة للميتاسبلويت

ls

cd metasploit-framework

msfconsole/.

_____

يمكن اختراق الأجهزة الذكية عبر العديد من الطرق والأساليب، ومن أهمها:

1- استغلال الثغرات الأمنية: قد يتم استغلال ثغرات في نظام التشغيل أو التطبيقات الموجودة على الجهاز، وهو ما يسمح للمهاجم بالوصول

إلى البيانات المخزنة على الجهاز.

2- الهجمات عن طريق الشبكة: يمكن للمهاجمين الدخول إلى شبكات الواي فاي التي يتصل بها الجهاز، وقد يتم استخدام أدوات الاختراق لتحيل الجهاز للاتصال بشبكة مشبوهة Wi-Fi مثل اختراق الشبكات وتزوير نقطة وصول.

3- الرسائل الاحتيالية: يمكن للمهاجمين إرسال رسائل احتيالية تحمل روابط ضارة أو ملفات مصابة بالفيروسات، وعندما يفتح المستخدم هذه الرسالة أو ينقر على هذه الروابط، يتم تنزيل برامج خبيثة على جهازه.

4- استخدام كلمات المرور الضعيفة: قد يتم اختراق الجهاز عن طريق الحصول على كلمات المرور الخاصة بصفحات التسجيل الخاصة بالجهاز، وبالتالي السيطرة على الجهاز بأكمله.

5- التطبيقات الخطرة: عندما يتم تحميل التطبيقات من مصادر غير رسمية أو غير موثوقة، فإن هذه التطبيقات يمكن أن تحتوي على برامج خبيثة.

اختبار الاختراق، والمعروف أيضًا باسم اختبار القلم، هو عملية تقييم أمان جهاز أو شبكة من خلال محاولة استغلال نقاط الضعف. إنها طريقة يستخدمها متخصصو الأمن السيبراني لتحديد نقاط الضعف في النظام قبل أن يتمكن المهاجم من استغلالها.

يمكن إجراء اختبار الاختراق باستخدام أدوات وتقنيات مختلفة، مثل فحص الثغرات الأمنية، ورصد الشبكات، والهندسة الاجتماعية، والاختبار المادي.

من حيث الشرعية، يُسمح عمومًا باختبار الاختراق طالما تم إجراؤه بالترخيص والموافقة المناسبين. ومن المهم الحصول على إذن من المالك أو المسؤول عن الجهاز أو الشبكة التي يتم اختبارها قبل إجراء أي اختبار اختراق. بالإضافة إلى ذلك، من الضروري اتباع جميع القوانين واللوائح المعمول بها عند إجراء اختبار الاختراق.

في بعض الحالات، قد يكون اختبار الاختراق مطلوبًا بموجب القانون، كما هو الحال في الصناعة المالية أو الأنظمة الحكومية. من المهم دائمًا التأكد من أن أي اختبار اختراق يتم إجراؤه يتم بطريقة قانونية ومسؤولة.

ما هي طرق اختراق أجهزة الكمبيوتر؟

1) التصيد الاحتيالي: تتضمن هذه الطريقة إرسال رسائل بريد إلكتروني احتيالية أو رسائل تبدو وكأنها من مصدر شرعي، بهدف خداع المستلم لمشاركة معلومات حساسة، مثل بيانات اعتماد تسجيل الدخول أو أرقام بطاقات الائتمان أو أرقام التعريف الشخصية.

2) البرامج الضارة: يمكن للمتسللين استخدام أشكال مختلفة من البرامج الضارة للوصول غير المصرح به إلى نظام الكمبيوتر. وتشمل هذه الفيروسات والديدان وأحصنة طروادة وبرامج التجسس، والتي يمكن تثبيتها على جهاز كمبيوتر من خلال مرفقات البريد الإلكتروني المصابة أو التنزيلات.

3) الهندسة الاجتماعية: تتضمن هذه الطريقة التلاعب بالأفراد لإفشاء معلومات حساسة أو تنفيذ إجراءات تمكن المتسلل من الوصول إلى نظام الكمبيوتر. يمكن أن تشمل تكتيكات الهندسة الاجتماعية الذريعة، والإغراء، والمقايضة.

4) هجوم القوة الغاشمة: تتضمن هذه الطريقة استخدام برنامج آلي للتخمين السريع أو "القوة الغاشمة" لكلمات المرور وبيانات اعتماد تسجيل الدخول حتى يتم التعرف على الكلمة الصحيحة.

5) حقن SQL: تتضمن هذه الطريقة استغلال الثغرات الأمنية في قاعدة بيانات موقع الويب للوصول إلى المعلومات الحساسة. يمكن للمتسلل إدخال تعليمات برمجية SQL ضارة في حقول البحث أو تسجيل الدخول بموقع الويب للوصول إلى قاعدة البيانات واسترداد المعلومات الحساسة أو تعديلها.

6) هجوم الرجل في الوسط: تتضمن هذه الطريقة اعتراض الاتصالات بين طرفين، مثل المعاملات المصرفية عبر الإنترنت أو تبادل البريد الإلكتروني، واستخدام تلك المعلومات للوصول إلى البيانات الحساسة أو إعادة توجيه الأموال إلى حساب آخر.

هناك عدة طرق لاختراق أجهزة التوجيه، بما في ذلك:

1. استغلال كلمة المرور الافتراضية: تأتي العديد من أجهزة التوجيه بكلمات مرور افتراضية يسهل تخمينها، مما يجعلها عرضة للاختراق.

2. الإصابة بالبرامج الضارة: يمكن أن تصيب البرامج الضارة جهاز التوجيه، مما يمنح المهاجم القدرة على التحكم في الشبكة.

3. هجوم الرجل في الوسط: يستطيع المتسلل اعتراض الاتصال بين جهاز التوجيه والأجهزة المتصلة، مما يسمح له بسرقة البيانات أو إدخال تعليمات برمجية ضارة.

4. استغلال الثغرات الأمنية: يمكن للمتسللين استغلال الثغرات الأمنية في البرامج الثابتة أو البرامج الخاصة بجهاز التوجيه للوصول إلى الشبكة.

5. الهندسة الاجتماعية: يمكن للمتسللين استخدام تقنيات الهندسة الاجتماعية لخداع المستخدمين للكشف عن بيانات اعتماد تسجيل الدخول أو غيرها من المعلومات الحساسة.

من الضروري الحفاظ على تحديث البرامج الثابتة لجهاز التوجيه الخاص بك واستخدام كلمات مرور قوية وفريدة لمنع هذه الأنواع من الهجمات.

هناك عدة طرق لاختراق أجهزة التحكم عن بعد، بما في ذلك:

1. الاستنشاق: يتضمن اعتراض الاتصال بين جهاز التحكم عن بعد والجهاز المستهدف، مثل التلفزيون أو مكيف الهواء.

2. إعادة تشغيل الهجمات: يتضمن ذلك تسجيل الاتصال بين جهاز التحكم عن بعد والجهاز المستهدف ومن ثم إعادة تشغيل البيانات المسجلة للتحكم في الجهاز.

3. التنصت: يتضمن مراقبة الاتصال بين جهاز التحكم عن بعد والجهاز المستهدف للوصول إلى عناصر التحكم في الجهاز.

4. العبث المادي: يتضمن العبث المادي بجهاز التحكم عن بعد للوصول إلى مكوناته الداخلية والتحكم بالجهاز مباشرة.

5. الهندسة الاجتماعية: تتضمن خداع مستخدم جهاز التحكم عن بعد للكشف عن رموز التحكم أو كلمات المرور الخاصة به، والتي يمكن بعد

ذلك استخدامها للتحكم في الجهاز.

ولكل طريقة من هذه الطرق مخاطرها وتحدياتها الخاصة، وتعتمد فعالية كل طريقة على الظروف المحددة والجهاز المستهدف.

ما هي أفضل طرق حماية الأجهزة من الاختراق؟

هناك عدة طرق لحماية أجهزتك من الاختراق، منها:

1. حافظ على تحديث برامجك وأجهزتك عن طريق تحديث نظام التشغيل والمتصفح والحماية من الفيروسات بانتظام.

2. استخدم كلمات مرور قوية وفريدة ومعقدة لجميع حساباتك وقم بتغييرها بشكل متكرر.

3. كن حذرًا عند استخدام شبكات Wi-Fi وتجنب الوصول إلى المعلومات الحساسة أثناء الاتصال بها العامة.

4. قم بتثبيت برنامج أمان موثوق يتضمن ميزات جدار الحماية ومكافحة البرامج الضارة ومكافحة برامج التجسس.

5. تجنب النقر على الروابط المشبوهة أو تنزيل المرفقات من مصادر غير معروفة.

6. استخدم المصادقة الثنائية كلما أمكن ذلك.

7. قم بمراقبة حساباتك بانتظام بحثًا عن أي نشاط مشبوه أو وصول غير مصرح به.

8. قم بعمل نسخة احتياطية لبياناتك بانتظام لمنع فقدان البيانات في حالة محاولة الاختراق.

باتباع هذه النصائح، يمكنك تقليل خطر تعرض أجهزتك للاختراق بشكل كبير.

ما هي أساليب اختراق الأجهزة الذكية وكيف يمكن حمايتها؟

الهندسة الاجتماعية: تتضمن هذه الطريقة خداع الأشخاص للكشف عن معلومات حساسة أو منح حق الوصول إلى أجهزتهم الذكية. 2. البرامج الضارة: يمكن زرع البرامج الضارة على الأجهزة الذكية من خلال رسائل البريد الإلكتروني التصيدية أو مواقع الويب المصابة أو تطبيقات الطرف الثالث. 3. هجوم الرجل في الوسط: يقوم المتسللون باعتراض الاتصالات بين طرفين لسرقة المعلومات. 4. نقاط الضعف في البرامج أو الأجهزة: يستغل المتسللون نقاط الضعف في كود الجهاز أو الأجهزة. لحماية الأجهزة الذكية، يجب على المستخدمين: 1. استخدام كلمات مرور قوية وفريدة وتمكين المصادقة الثنائية. 2. قم بتحديث البرامج والبرامج الثابتة بانتظام. 3. تجنب النقر على الروابط المشبوهة أو تنزيل التطبيقات المشكوك فيها. 4. كن حذرًا بشأن مشاركة المعلومات الشخصية.

ما هي أهم طرق اختراق الأجهزة الذكية؟

لإجابة على هذا السؤال، سأزودك ببعض الأساليب الأكثر شيوعًا التي يستخدمها المتسللون لاختراق الأجهزة الذكية:

1. استغلال كلمات المرور الضعيفة: يمكن الوصول إلى العديد من الأجهزة الذكية عبر الإنترنت، مما يعني إمكانية التحكم بها عن بعد أو البلوتوث. يمكن للمتسللين استخدام نقطة الوصول هذه لاستغلال كلمات المرور الضعيفة والتحكم في الجهاز Wi-Fi باستخدام شبكة.

2. نقاط الضعف في البرامج الثابتة: غالبًا ما تحتوي الأجهزة الذكية على برامج ثابتة يمكن تحديثها لإصلاح مشكلات الأمان. ومع ذلك، إذا لم يتم تثبيت هذه التحديثات، فقد يكون الجهاز عرضة للهجوم.

3. هجمات التصيد الاحتيالي: يمكن للمتسللين استخدام هجمات التصيد الاحتيالي لخداع المستخدمين للتخلي عن معلومات تسجيل الدخول الخاصة بهم أو البيانات الحساسة الأخرى. يمكن القيام بذلك من خلال رسائل البريد الإلكتروني أو الرسائل النصية أو حتى المكالمات

.الهاتفية

4. هجمات الهندسة الاجتماعية: يمكن للمتسللين استخدام هجمات الهندسة الاجتماعية لخداع المستخدمين للتخلي عن معلومات تسجيل الدخول الخاصة بهم أو البيانات الحساسة الأخرى. يمكن القيام بذلك من خلال رسائل البريد الإلكتروني أو الرسائل النصية أو حتى المكالمات الهاتفية.

5. هجمات البرامج الضارة: يمكن للمتسللين استخدام البرامج الضارة لإصابة الأجهزة الذكية والتحكم فيها. ويمكن القيام بذلك من خلال مرفقات البريد الإلكتروني، أو التنزيلات من مواقع الويب غير الجديرة بالثقة، أو حتى من خلال الوصول الفعلي إلى الجهاز.

بشكل عام، فإن الطريقة الأكثر أهمية لاختراق الأجهزة الذكية هي استغلال نقاط الضعف في أمانها. من خلال الحفاظ على تحديث أجهزتك الذكية، واستخدام كلمات مرور قوية، والوعي بهجمات التصيد الاحتيالي أو هجمات الهندسة الاجتماعية المحتملة، يمكنك المساعدة في حماية نفسك من هذه الأنواع من الهجمات.

هجمات ما قبل االتصال Attacks connection-Pre

:فيما يلي الخطوات ألساسية التي سنجريها لتنفيذ هجوم ما قبل االتصال

1. واجهة السلكية في وضع مراقب: في هذه الخطوة، سوف نقوم بتغيير وضع

.الجهاز الالسلكي كوضع مراقب

2. في هذه الخطوة، سوف نستخدم :ng-airodump حول أو عن أداة

.لسرد جميع الشبكات من حولنا وعرض معلومات مفيدة عنها ng-airodump

3. في هذه الخطوة، سنرى جميع ألجهزة المتصلة :ng-airodump تشغيل

بشبكة معينة ونجمع ا

ً

.مزيد من المعلومات عنها

4. مصادقة العميل الالسلكي: في هذه الخطوة، يمكننا فصل أي جهاز يظهر في

.ng-aireplay الخطوة السابقة باستخدام

:واجهة السلكية في وضع مراقب

ستخدمُ

.ت هذه الخطوة لوضع بطاقتنا الشبكية الالسلكية في وضع المراقب

في وضع المراقب، يمكن أن تستمع بطاقتك إلى كل الحزم الموجودة حولنا. بشكل مما يعني ،("Managed(افتراضي، يتم تعيين االجهزة الالسلكية على وضع " إدارة الخاص MAC أن جهازنا الالسلكي لن يلتقط سوى الحزم التي تحتوي على عنوان الوجهة. سيتم فقط التقاط الحزم التي هي في الواقع مرسلة MAC بجهازنا باعتباره لجهازنا فقط

.لسرد جميع الشبكات من حولنا وعرض معلومات مفيدة عنها ng-airdump يستخدم لذا فهي مصممة بشكل أساسي اللتقاط جميع الحزم من ،(sniffing(إنها حزمة شم حولنا بينما نحن في وضع المراقب. يمكننا تشغيلها على جميع الشبكات من حولنا واسم القناة ونوع التشفير وعدد العمالء mac وجمع معلومات مفيدة مثل عنوان ض المتصلين بالشبكة ثم البدء في استهداف الشبكة الهدف. يمكننا اً أي تعيينها على

.المعينة Fi-Wi حتى ال نلتقط سوى الحزم من شبكة الـ(AP(نقطة وصول معينة

:بناء الجملة

airodump-ng [MonitorModeInterface]

Fi-Wi أوالً، لنل ق نظرة على كيفية تشغيل االداة. في هذه الحالة، نحتاج إلى بطاقة .wlanلدينا هو Fi-Wi 0 في وضع المراقبة. اسم بطاقة

root@kali:~# airodump-ng wlan0

---]15[----------

.إليقاف التنفيذ C + Ctrl مالحظة: يمكننا الضغط على

:حيث

.للشبكة المستهدفة MAC عنوان : BSSID

.قوة إشارة الشبكة. كلما كان أكبر كان أفضل : PWR

.هي: اإلطارات التي ترسلها الشبكة من أجل بث وجودها Beacons

ُظهر : #Data

ي عدد حزم البيانات أو عدد إطارات البيانات المستخدمة حاليا.

ظهر : /#s ُ

ي عدد حزم البيانات التي نجمعها في الثواني العشر الماضية.

يعرض CH: القناة التي تعمل عليها الشبكة.

يظهر ENC : التشفير المستخدم من قبل الشبكة. يمكن أن يكون OPN، WEP، WPA، 2WPA.(بمعنى التشفير encryption اختصار لـ)

يظهر CIPHER : الشفرات المستخدمة في الشبكة.

يعرض AUTH : المصادقة المستخدمة على الشبكة.

يعرض ESSID : اسم الشبكة.

في الصورة السابقة، يمكنك رؤية جميع الشبكات الالسلكية مثل perfe و Oppo و Flight و Ashu و LIFCA و Xiaomi و BS1A-YW5 ومعلومات ،وغيرها مفصلة حول جميع الشبكات.

ا ng-airodump أي لتحديد جميع األلجهزة المتصلة بأيً ض مالحظة: يستخدم شبكة تكون في نطاقنا.

إليقاف التنفيذ C + Ctrl مالحظة: يمكننا الضغط على.

حيث:

BSSID : عنوان MAC للشبكة المستهدفة.

PWR : قوة إشارة الشبكة. كلما كان أكبر كان أفضل.

Beacons هي: اإلطارات التي ترسلها الشبكة من أجل بث وجودها.

ظهر : #Data ُ

ي عدد حزم البيانات أو عدد إطارات البيانات المستخدمة حاليا.

ظهر : /#s ُ

ي عدد حزم البيانات التي نجمعها في الثواني العشر الماضية.

يعرض CH: القناة التي تعمل عليها الشبكة.

يظهر ENC : التشفير المستخدم من قبل الشبكة. يمكن أن يكون OPN، WEP،

)بمعنى التشفير encryption اختصار لـ).WPA، 2WPA

.الشفرات المستخدمة في الشبكة : CIPHER يظهر

.المصادقة المستخدمة على الشبكة : AUTH يعرض

.اسم الشبكة : ESSID يعرض

و perfe و Oppo في الصورة السابقة، يمكنك رؤية جميع الشبكات الالسلكية مثل

Flight و Ashu و LIFCA و Xiaomi و BS1A-YW5 ومعلومات ،وغيرها

.مفصلة حول جميع الشبكات

تشغيل run airodump-ng airodump-ng

لرؤية جميع ألجهزة المتصلة بشبكة ng-airodump في هذه الخطوة، سنقوم بتشغيل

معينة وجمع المزيد من المعلومات عنها. بمجرد أن يكون لدينا هدف)شبكة(، من

،على تلك الشبكة فقط ng-airodump بدالً من تشغيلها على جميع المفيد تشغيل

.الشبكات من حولنا

ا،

ً

على جميع الشبكات من حولنا. سنستهدف آلن ng-airodump حالي نقوم بتشغيل

الشبكة BS1A-YW5 هو عنوانها يكون التي C8: E5: AF: F6: 33 :سنقوم .50

.باستنشاق تلك الشبكة فقط

:للقيام بذلك، سوف نستخدم نفس ألداة. سيكون ألمر كما يلي

root@kali:~# airodump-ng --bssid 50:C8:E5:AF:F6:33 --

channel 6 --write test wlan0

:حيث

🕐 --bssid 50: C8: E5: AF: F6: 33 عنوان هو MAC لنقطة

.الوصول. يتم استخدامه للقضاء على حركة المرور الغريبة

🕐 --channel 11 الستنشاق قناة هي airodump-ng.

يستخدم لتخزين جميع البيانات، في هذا المثال سيكون في ملف --write 🕐

أنها ليست إلزامية، يمكنك تخطي هذا الجزء .test يسمى.

🕐 0wlan هو اسم الواجهة، حاليا هي في وضع المراقب.

حيث:

🕐 BSSID : نفسه مكرر، ألننا في داخل هذه الشبكة.

🕐 STATION : عدد االجهزة المتصلة بهذه الشبكة.

🕐 PWR : يوضح قوة اإلشارة عند كل جهاز.

🕐 Rate : معدل السرعة.

🕐 lost : مقدار فقدان البيانات.

🕐 Frames : عدد اإلطارات التي قمنا بالتقاطها.

وجميع االجهزة لها YW-A1BSبعد تنفيذ هذا االمر، لدينا 3 أجهزة متصلة بشبكة 5

نفس BSSID مثل 50: 33 :F6 :AF :E5 :C8.

مصادقه العميل الالسلكيه

Deauthenticate the wireless client

ومن الهجمات المعروفة أيضا ما يعرف باسم هجمات المصادقة. هذه الهجمات مفيدة

جدا. تتيح لنا هذه الهجمات فصل أي جهاز عن أي شبكة تقع ضمن نطاقنا حتى إذا

كانت الشبكة بها تشفير أو تستخدم ا

ً

. مفتاح

في هجوم المصادقة، سوف نتظاهر بأننا عمالء ونرسل حزمة مصادقة إلى جهاز

الخاص بالعميل MAC الخاص بنا إلى عنوان MAC التوجيه عن طريق تغيير عنوان

وا الموجه أننا نريد قطع االتصال بك. في الوقت نفسه، سوف نتظاهر بأننا جهاز خبار

الخاص بالموجه MAC الخاص بنا إلى عنوان MAC توجيه عن طريق تغيير عنوان

حتى يتم فصل العميل الذي نطلبه. بعد هذا، سيتم فقد االتصال. من خالل هذه

العملية، يمكننا فصل أو مصادقة أي عميل من أي شبكة. للقيام بذلك، سوف نستخدم

أداة تسمى ng-aireplay.

على الشبكة الهدف، ألننا نريد معرفة ng-airodump قبل كل شيء، سنقوم بتشغيل

لذلك سنقوم -- writeالعمالء أو االجهزة المتصلة بها. هذه المرة، لن نحتاج إلى خيار

سنقوم بفصل الجهاز ،ng-airodump بإزالته. بعد االنتهاء من عملية تشغيل

بالمحطة A8: 7D: 12: 30: E9: A4 باستخدام aireplay-ng.

بناء الجملة:

root@kali:~# aireplay-ng --deauth [#DeauthPackets] -a

[NetworkMac] -c [TargetMac] [Interface]

-c ثم عنوان ماك الشبكة ثم– a ثم عدد الحزم ثم --deauth أكتب اسم االداة ثم

ثم عنوان ماك الهدف ثم اسم الواجهة.

root@kali:~# aireplay-ng --deauth 100000 –a

50:C8:E5:AF:F6:33 –c A8:7D:12:30:E9:A4 wlan0

فقد االتصال ،8:A :D7 :بعد تنفيذ هذا االمر، فإن الجهاز الذي تكون محطته 30 12

باإلنترنت. ال يمكنه االتصال بالشبكة مرة أخرى إال عند إنهاء هذا االمر التنفيذي

بالضغط على C + Ctrl.

حيث:

بأننا نريد تشغيل هجوم المصادقة وتعيين ng-airplay إلخبار --deauth 🕐

و هو عدد الحزم بحيث يستمر في إرسال حزم المصادقة إلى كل من 100000

جهاز التوجيه والعميل والحفاظ على العميل مفصوًال.

AF 5:E 8:C: لجهاز التوجيه. :50 MAC لتحديد عنوان -a يتم استخدام 🕐

هي نقطة الوصول الهدف 6:F 33.

🕐 c- عنوان يحدد MAC للعميل. A8: 7D: 12: 30: E9: A4 عنوان هو

للعميل MAC.

هو المحول الالسلكي، ال زال في وضع المراقب 0wlan 🕐.

المرحلة الثانية في االختراق

الوصول Gaining Access

هجوم الوصول: هو الجزء الثاني من اختبار اختراق الشبكة. في هذا القسم، سنتصل بالشبكة. سيتيح لنا ذلك شن هجمات أكثر قوة والحصول على معلومات أكثر دقة. إذا لم تستخدم الشبكة تشفير، فيمكننا فقط االتصال بها واستنشاق البيانات غير المشفرة.

إذا كانت الشبكة سلكية، فيمكننا استخدام كابل واالتصال بها، ربما من خالل تغيير الخاص بنا. *هذا ما ذكر عن الش باكت املفتوحة يف املوقع، لكن سأرفق MAC عنوان لمك يف هناية هذا الكتاب كيفية ذكل* المشكلة الوحيدة هي عندما يستخدم الهدف

إذا واجهنا بيانات مشفرة، نحتاج إلى معرفة WEP، WPA، 2WPA. تشفير مثل مفتاح فك تشفيرها، هذا هو الغرض الرئيسي في هذا الفصل.

إذا كانت الشبكة تستخدم تشفير، فال يمكننا الوصول ألي شيء ما لم نفك تشفيره.

سنناقش في هذا القسم كيفية كسر هذا التشفير وكيفية الوصول إلى الشبكات سواء تستخدم كانت WEP / WPA / WPA2.

سيغطي هذا القسم المواضيع التالية:

0- مقدمة WEP

1- أساسيات تكسير WEP

2- هجوم المصادقة الوهمية (ARP)

3- هجوم إعادة الطلب

4- نظرية المصافحة نظرية WEP-

5- إنشاء قائمة كلمات التقاط المصافحات 6- 7-

9- تأمين الشبكات من الهجمات التكسير بقائمة الكلمات -